IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, LLC, Plaintiff, v. CISCO SYSTEMS, INC., Defendant.	Case No.: 2:18-cv-00094-EWH-LRL **REDACTED - PUBLIC VERSION**

REPLY MEMORANDUM IN FURTHER SUPPORT OF PLAINTIFF'S MOTION FOR ADDITIONAL AND AMENDED FINDINGS AND AMENDED JUDGMENT UNDER RULE 52(b) OR, IN THE ALTERNATIVE, FOR A NEW TRIAL UNDER RULE 59(a)(2)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTRODUCTION

Cisco's opposition (Dkt. No. 800, "Opp.") fails to refute Centripetal's arguments that the Court's judgment of non-infringement rested on clear errors of law and fact that, if corrected, would compel entry of a new judgment in Centripetal's favor. *See* Fed. R. Civ. P. 52(b). At the very least, the Court should reopen the judgment and receive additional testimony and briefing regarding novel claim constructions and factual findings that the Court adopted without adequate notice to the parties. *See* Fed. R. Civ. P. 59(a)(2). While these are unusual remedies, this was an unusual case involving a virtually unprecedented use of Rule 63 to adjudicate highly technical issues based on a voluminous record of a trial held by a different (now-deceased) judge. Under these extraordinary circumstances, reconsideration is amply warranted. In seeking to avoid this conclusion, Cisco distorts Centripetal's Motion, the record, and the law.

ARGUMENT

I. THE '193 PATENT

A. The Court Should Correct Its Erroneous Construction of Claims 18 and 19 of the '193 Patent, Which Disclose Filtering of "Particular Type[s] of Data Transfer" Between Networks, Not Between Individual Computers

Cisco does not dispute that the '193 Patent discloses filtration of a subset of data transfers between *networks*. Opp. at 2-6. Indeed, both parties applied this construction at trial. *See, e.g.*, Tr. 490:17-491:2, 2400:8-10. Cisco nonetheless argues in its Opposition that the Court's contrary construction—requiring "filtration of a subset of packets sent between *computers* in two different networks," Op.[1] at 24 (emphasis added)—did not alter the claim scope or inform its non-infringement finding. Cisco is wrong.

[1] Memorandum Opinion and Order, Dkt. No. 780.

To prove infringement, the Court required Centripetal to establish that Cisco's Switches and Routers[2] block a subset of communications between two *computers* (rather than between two *networks*). The Court found the '193 Patent not infringed because "[t]he evidence does not show that a subset or portion of the packets—either from a quarantined computer to a restricted destination or from a quarantined computer to a permitted destination—can be dropped while other packets to that same destination are allowed." Op. at 23-24 (claims "require . . . filtration of a subset of packets sent between computers in two different networks."). In other words, while the claims disclose the forwarding and dropping of packets from any number of computers in the first *network* to any number of computers in the second *network*, the Court's construction requires the *same computer* in the first network to forward and drop packets to another *singular computer* in the second network. Op. at 23-24. To be sure, the Court understood that a network includes multiple computers, *see* Opp. at 2-3, and the data packets at issue "must originate from one or more 'computers'" *Id.* at 5. But none of that alters the bottom line: The Court erroneously limited Centripetal's claims to communications between *one computer* and *a second computer*, rather than between *one network* and *a second network* (each consisting of many computers).[3] Correcting this erroneous narrowing of the claim scope would require entry of an amended judgment in Centripetal's favor.

Cisco seeks to avoid this result by asserting that the Court's decision did not depend on this construction. That effort goes nowhere. The Court's analysis turned on whether Cisco's

[2] Terms defined in Centripetal's Memorandum in Support of its Motion (Dkt. No. 791) have the same meaning herein.

[3] Cisco's citations are likewise irrelevant. Cisco cites a PowerPoint slide from its technology tutorial showing that a network has multiple computers, but it does not discuss the claim language of the '193 Patent. Cisco also tries to argue about a different claim element, which states "receive, from a computing device located in a first network, a plurality of packets," Opp. at 3 (citing '193 Patent at claims 18 and 19), but Cisco did not dispute infringement of this element.

accused products "drop some, but not all, packets sent between two different network *destinations*"—*i.e.*, between two different *computers* (in different networks). Opp. at 3 (emphasis added) (quoting Op. at 24). And Centripetal assuredly *does* "challenge that understanding," *contra* Opp. at 3; the correct inquiry is instead whether the accused products drop some, but not all, packets sent between two different *networks*. *See* '193 Patent, Claims 18 and 19 (describing "packet-filtering rules configured to prevent a particular type of data transfer from [*a*] *first network* to *a second network*") (emphasis added). As Centripetal's Motion explained, giving effect to plain meaning of "first network" and "second network" leads to a straightforward finding of infringement here, as Cisco's Switches and Routers are capable of blocking a subset of data transfers from one network—namely those transfers from computers that have been assigned a "quarantine" SGT tag—while allowing other transfers (that have not been assigned a quarantine "SGT" tag) from other computers on that network to go through. *See* Mot. at 8.

It is obviously important as a legal matter that the Court stay true to the claims as written, because (as explained above) doing so would result in a finding of infringement. It is also critical in the real world. The reason the '193 Patent claims recite transfers between networks (and not computers) is that the Switch or Router may not know the original source or destination of the traffic because of Network Address Translation ("NAT"), which (as the Court is aware) changes the IP addresses of packets to hide the computers that are in the network, particularly when each network is protected by a firewall. Because the Switch or Router may only know the IP address of a firewall protecting a network (rather than the individual computers on the network), the Switches and Routers also analyze the traffic to determine if it is tagged so that the Switch and Router can block traffic even if the IP address of the firewall is permitted.

Unable to dispute this basic reality or that the Court's construction contradicts the claims, Cisco argues that this is a "new" infringement theory and insists that a new trial is needed to address it. But Cisco simply mischaracterizes Centripetal's argument. Contrary to Cisco's characterization, *see* Opp. at 6, Centripetal argues here, just as it did at trial and the Rule 63 hearing, that the claims require the analysis of traffic *between networks*, and that *some* traffic that has been quarantined will be blocked while other traffic is allowed. *See* Mot. at 6-8; Tr. 468:8-17, 489:22-490:16, 518:22-520:13, 521:8-522:21; R.63 Tr. 237:3-239:6. In short, Cisco's Switches and Routers plainly infringe under the correct construction of "particular type of data transfer from the first network to a second network" because those devices block a subset of data transfers (those that have been assigned a "quarantine" SGT tag) and allow others (those without an SGT tag). *See* Mot. at 8 (citing testimony and exhibits). The Court should amend its findings to correct the erroneous construction of the "particular type of data transfer" limitation and conclude that Cisco's Switches and Routers infringe the '193 Patent.

B. At the Very Least, the Court Should Hold Additional Proceedings on Its New Construction

If the Court declines to amend its judgment to enter a finding of infringement by Cisco, it should reopen the judgment to permit Centripetal to prove infringement under the Court's new construction of the claims.

Cisco notably does not dispute that the law requires an opportunity to address a court's new claim construction. *Cf.* Mot. at 9 (citing cases). And while Cisco asserts that there is no need to allow evidence on micro-segmentation to prove infringement under the Court's new construction, *none* of the supposedly overlapping testimony that Cisco cites mapped micro-segmentation or segmentation to the new requirement that the particular type of data transfer be

between two computers.[4] *See* Opp. at 9-10 (citing, *e.g.*, R.63 Tr. 164:5-168:17, 251:4-8, 265:21-268:10). Furthermore, Cisco ignores the documents that were not admitted at the Rule 63 hearing or at trial. Mot. at 10-11 (citing, *e.g.*, Cisco's websites on micro-segmentation); *see* R.63 Tr. 188:14-19 (the Court declined to admit the web page printouts in Dr. Almeroth's cross examination).

Finally, Cisco is incorrect that the parties need to redo the entire case for some "unspecified rules." Opp. at 10. Rather than restart from scratch, further proceedings would be narrowly focused on whether Cisco's products infringe under the Court's new interpretation that the claims require blocking a "particular type of data transfer" between two *individual computers*.[5]

C. The Court Should Also Correct Its Erroneous Description of the Accused Products

Reconsideration is also warranted because the Court's ruling rests on an incorrect understanding of how Cisco's Switches and Routers operate. The record makes clear that these accused products decide whether to forward or drop packets in two steps. First, the Switch or Router checks the destination IP address to see whether the packet *can* be forwarded to the destination as specified by the ACL rules, *i.e.*, the packet is destined for a network that is connected to the Switch or Router and is allowed to be forwarded. If the destination IP address is permitted, the process continues to the next step; if not, it is dropped. Tr. at 537:15-24 (explaining PTX-1390 at 0086), 538:7-16; *see also* PTX-1276 at 0216. Second—if the destination network is connected and permitted—the Switch or Router checks to see whether it *should* transfer the packet or if it is

[4] Notably, an architecture in which two networks are protected by firewalls and connected to each other by a Router also satisfies the Court's new construction of a particular type of data transfer because a subset of the traffic coming from the firewall (which is a computer) to the Router will contained tagged traffic while other traffic from the same firewall to the Router will not contain tagged traffic.

[5] For example, Centripetal will be showing how micro-segmentation will infringe. Mot. at 10-11.

potentially malicious, which it does by checking for an SGT tag (*i.e.*, a quarantine tag) as specified by the SGACL rule.[6] If the packet is tagged, it is dropped; if not, it is forwarded. Tr. 530:4-531:21 (discussing PTX-563 at 415); R.63 Tr. at 157:8-19, 160:3-20; PTX-1390 at 0086, PTX-1280 at 0021; *see* Mot. at 11-12.

Cisco does not dispute that this is how its Switches and Routers technology works. Nor does it dispute that the Court found, *contrary to how the technology actually works*, that Switches and Routers perform a quarantine with a simple destination check, rather than based on the particular type of transfer. *See* Opp. at 11-12. That alone confirms that the judgment cannot stand.

Both parties' experts agreed that SGT and SGACL check the type of data transfer, which is different from the simple destination check. *See, e.g.*, Tr. 494:3-24, 498:4-19 (Dr. Mitzenmacher testified that the SGT and SGACL are based on the role of the computer), 2390:18-24 (Cisco's expert Dr. Crovella also testified that the SGACL "will filter traffic based on the role of the device"); R.63 Tr. 157:8-19 (reading from PTX-1276 at 0211: "Because SGACL is role based, not based on individual IP addresses or MAC addresses, it significantly simplifies access control."), 160:3-20 (Cisco's expert Dr. Almeroth agreed that when applying the SGACL rules, it looks at the tags, not looking at the IP address); *see also* PTX-1280 at 0021 (example SGACL rules based on the SGT tag value 255); Tr. 531:16-21, 496:19-497:4, 497:14-498:19. No evidence supports Cisco's effort to collapse the two checks into one.

Unable to find evidence supporting the Court's misconstruction, Cisco resorts to misstating the record. First, Cisco takes out of context Dr. Mitzenmacher's explanation of a *typical policy* that "restrict[s] according to source and destination." Opp. at 11 (citing Tr. 528:3-4).

[6] SGACL is not "the only accused rule." *Contra* Opp. at 11. SGACL is discussed only in the context of the "particular type of data transfer" element, which is the sole disputed element. *See, e.g.*, PTX-1280 at 0021 (discussing SGACL); PTX-1390 at 0086 (showing processing with ACLs).

Dr. Mitzenmacher plainly was not discussing SGT, SGACL, or the "particular type of data transfer" element. Rather, he was addressing a hypothetical question from the Court. Tr. 530:1-2. Later, Dr. Mitzenmacher returns to his testimony and explains how the Centripetal technology is superior because it prevents exfiltration from protected networks but still allows communications to unprotected networks, just as the claims require. Tr. 530:3-24. Cisco also distorts Centripetal's record citations—which actually state that SGACL checks the role of an endpoint computer (*i.e.*, by checking the SGT tag) to restrict access, rather than (as Cisco argues) that SGACLs restrict access (*i.e.*, drop packets) based only on the destination IP address.[7] Tellingly, Cisco has no answer for the fact that SGACLs would be entirely redundant if they were only destination-based. *See* Mot. at 2-12; Opp. at 11-12. Cisco does not explain how its Switches and Routers can effectuate a quarantine based solely on a source and destination check with no visibility into the type of data transfer. That is because it cannot.

Cisco's opposition tries to elide the distinction between access restriction and a destination check. *See* Opp. at 11-12. But the record definitively shows that Cisco's quarantine rules (with SGT and SGACL) restrict access by performing more refined filtering packets based on the tag applied to the packet (*e.g.*, type of data transfer and the presence of potentially malicious activity

[7] Cisco resorted to mischaracterization of evidence to support its position that SGT/SGACL only checks the destination. Contrary to Cisco's characterization, Dr. Mitzenmacher actually testified that quarantine rules only block access to certain parts of a network (rather than an entire network). *See* Tr. 468:8-17, 535:21-24 (parts of the internal networks are still allowed). Similarly, the evidence identified in Cisco's brief (at Opp. at 12) states that SGT/SGACL are role-based (*i.e.*, rather than being based on source or destination), rather than destination-based, as Cisco contends. *See, e.g.*, PTX-1280 at 0021 (SGT and SGACL use "role-based permissions" to limit particular traffic as it flows through a network); Tr. 496:12-499:16 (Dr. Mitzenmacher's discussing the change of group numbers as part of changing role-based permissions to prevent data exfiltration). Cisco's attorney also distorted Dr. Mitznemacher's testimony and the document, which in fact shows that SGACL is applied last, *after* the other ACLs (such as RACL) already checked the source and destination. *See* R.63 Tr. 306:1-25; PTX-1390 at 0086. Finally, whether PTX-1193 is prior art is irrelevant since Cisco failed to show its alleged prior art teaches the '193 Patent.

per the SGT tag)—*not* destination (*e.g.*, IP addresses). *See, e.g.*, Tr. 535:3-17 (Switches and Routers look at SGT tag in addition to other fields, such as IP addresses in the header to drop packets); PTX-1276 at 0216 (describing RACL which provides destination IP address check before the Group ACL); PTX-1288 at 0012 (similar); PTX-1390 at 0086 (SGACL is applied last after all other ACLs), PTX-1280 at 0021 (showing SGT number which is not a destination address); PTX-1326 at 0011 (describing changing *users'* access privilege); Tr. 468:8-17 (a computer being used may reach some destinations, but not others, within an internal network); Tr. 489:17-490:16 (user nay access only certain parts of an internal network if the user is suspicious); Tr. 494:12-24 ("So if you've found a user that's suspicious you might say, okay, I'm going to apply this [SGT], in particular a quarantine tag . . . ."); Tr. 538:7-16, 2389:1-8; Tr. 467:10-468:17 (explaining that Switches and Routers can prevent access to certain parts of the internal network based on the role of the endpoint device); PTX-1280 at 0021 (showing security group numbers which represent the role of devices in that group); Tr. 489:17-490:16 (user nay access only certain parts of an internal network if the user is suspicious).

In short, the Court's non-infringement conclusion was premised on a fundamental misunderstanding of the functionality of the accused devices. It should be corrected in an amended judgment of infringement of the '193 Patent. At the very least, the judgment should be reopened and the Court should hold additional proceedings consistent with the above.

II. THE '806 PATENT

A. Cisco's Opposition Confirms that the Court Ruled for Cisco Only Because It Misapprehended Cisco's Technology and Centripetal's Infringement Theory

As Centripetal's Motion explains, the Court erred by assessing how Cisco's products operate in their normal mode, during which there is an extremely brief "idle period" between the processing of each packet, instead of how they work in the special rule-swapping mode where

there is no such idle period and the products cache packets (to avoid dropping them) while a new rule set is substituted for an older set. *See* Mot. at 15-19. Cisco's opposition only confirms that the Court's judgment rests on a misunderstanding of both Cisco's technology and Centripetal's infringement theory.

Cisco leads off by asserting that the Court properly "compare[d] packet processing during normal operations . . . with packet processing during the rule swap . . . ." Opp. at 12-13. But Cisco glosses over the substance of that comparison, particularly the Court's reliance on the fact that the accused products "cease processing packets, albeit very briefly" during an "idle period" of two to four clock cycles. Op. at 37. As Centripetal has explained, this "idle period" exists only *during normal packet processing* and is not what meets the '806 Patent's requirement to "cease processing" packets *during a rule-swap*; instead, that requirement is satisfied because "there is no processing of any packets" when the accused products are in rule-swapping mode. Mot. at 15-16; *see also, e.g.*, Tr. 606:6-608:9, 616:15-617:18, 841:8-22; PTX-1915. Cisco offers no defense of the Court's analysis on this point, effectively conceding that the Court's focus on "idle periods" was misguided. *See, e.g.*, Mot. at 18 ("By focusing on 'idle' time during normal processing rather than on what occurs during the rule swap process, the Court mistook Centripetal's infringement case.").

Cisco next asserts that its accused products make "no changes to packet processing during [a] rule swap . . . ." Opp. at 13-14 ("[T]he only change that occurs as a result of a rule swap is that one packet is processed according to the old rule set . . . ."). But there is extensive record evidence showing that Cisco's devices do not process *any* packets in rule-swapping mode; processing resumes only when the rule-swap is completed. *See, e.g.*, Tr. 606:6-608:9, 616:15-617:18, 631:14-632:9 (Mitzenmacher testimony); PTX-1195 (describing Hitless ACL); PTX-1196 (describing

Transactional Commit Model); PTX-1915 (Jones testimony). [redacted] *See* Tr. 635:22-638:17, 867:13-868:19; *see also id.* 1651:23-1652:6 (the Court noting that "you can't be processing packets at the same time as you change rules."), 2520:21-2522:17 (the Court noting that there is "some time" to switch rule sets). Cisco ignores all of this record evidence. Instead, Cisco points to a single marketing document that states that Hitless ACL is performed "without interrupting traffic." Opp. at 14-15 (quoting PTX-1303 at 0073). But that document lends no support to Cisco's claim that the accused products continue processing packets while in rule-swapping mode. Nor could it: *Cisco's own engineer* testified that that "without interrupting traffic" means that packets are cached during a rule swap instead of being dropped.[8] Tr. 2552:18-25; *see also* PTX-1915 (noting that packets are not dropped using Hitless ACL, *i.e.*, they are cached).

Cisco's argument that "the default is not 'to drop packets,'" Opp. at 16, is likewise unavailing. Cisco again points to its marketing document, this time citing a statement that "Hitless update is enabled by default" and "can't be disabled." *Id.* at 16 (quoting PTX-1303 at 0073). [redacted] *See* PTX-1195 at 4 (Step 7); PTX-1849 at 21, 29. Whether the technology can be "disabled" is totally beside the point.

[8] Contrary to Cisco's assertion, the operation of its old system is not irrelevant, as it shows that 1) rule swapping is not part of the normal processing of packets, as the old system dropped packets despite having a cache, 2) [redacted] and 3) the preprocessing of rules allows for the quick swapping of rules that in turn allows the Switches and Routers to cache packets and resume processing quickly. *See* Mot. at 14-18.

Cisco also has no answer for the wealth of evidence—including, most notably, *its own internal documents and source code*—showing that the accused products enter this rule-swapping state in response to a signal, just as Claims 9 and 17 of the '806 Patent describe. As Centripetal has explained, that signal is provided in Step 7 of Hitless ACL for Switches and Routers and the Transactional Commit Model for Routers. *See* Mot. at 16-18. None of Cisco's witnesses, including Mr. Shankar and Mr. Jones, and its expert, Dr. Reddy, addressed the underlying documents or source code that Centripetal and its expert witness relied upon. Dkt. No. 725 (Centripetal's FoF) at ¶¶ 256-257.

Lacking a persuasive response to the substance of Centripetal's arguments, Cisco tries to cast them as "new." Opp. at 14-15. But Centripetal repeatedly asserted—and developed a record to establish—that rule swapping differs from (and interrupts) normal packet processing. *See, e.g.*, Dkt. No. 725 (Centripetal's FoF) at ¶¶ 247-257, 269-271, 273-281, 294-300; Tr. 606:6-608:9, 616:15-617:18, 635:22-638:17, 631:14-632:9, 867:4-868:19; PTX-1195; PTX-1196; PTX-1915. [redacted]. *See, e.g.*, PTX-1195 at 4; PTX-1849 at 21 (lines 568-606), 29 (line 2742); Tr. 508:6-509:4, 639:4-25; *see also* Dkt. No. 725 (Centripetal's FoF) at ¶¶ 253-254, 280-281, 299-300, 326. [redacted]. *See, e.g.*, Tr. 508:6-509:4, 639:3-25.

In sum, the accused network devices receive a signal that causes them to switch from their normal packet processing mode to a rule-swapping state in which they cache packets (to avoid dropping them), switch the rule sets, and signal that the swap is complete—just as the asserted

claims describe. This Court should correct its contrary finding, which is not supported by the record, and enter an amended judgment for Centripetal.

B. The Court Erred in Construing the Claims' Requirement to "Cease Processing" Packets During a Rule Swap

Cisco's opposition also fails to refute Centripetal's alternative argument that the Court erred in removing the first (old) rule set from the context of the '806 Patent's requirement to "cease processing of one or more packets." *See* Mot. at 19-20. In context, this phrase indicates that the device stops processing incoming packets using the old set of rules, and instead "cache[s]" these packets while it is "reconfigured to process packets in accordance with the second rule set." '806 Patent at 8:66-9:19, 7:57-8:23. Indeed, Cisco's own experts (namely Dr. Reddy and Dr. Almeroth) confirmed that "ceasing processing of one or more packets" means "[s]top processing packets with *first* rule set." Ex. A, Reddy Demonstrative at 43 (emphasis in original); R.63 Tr. 199:18-201:1 ("So packets should stop being processed according to the *first rule set* and then some additional steps should happen.") (emphasis added). Dr. Mitzenmacher said the same thing: He testified that when signaled, the accused products "stop processing" *using the first rule set*. Tr. 617:7-15, 621:19-622:3 (testifying to "stop processing," do a "swap-over" and "move on using the second rule set"). Cisco's argument thus fails for a fundamental reason: While a claim cannot be construed in a way that contradicts its plain text, Centripetal's reading (embraced by Cisco's own experts) creates no such contradiction.

Cisco cannot dispute that "a claim interpretation that excludes a preferred embodiment from the scope of the claim is rarely, if ever, correct." *Accent Packaging, Inc. v. Leggett & Platt, Inc.*, 707 F.3d 1318, 1326 (Fed. Cir. 2013); *accord Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) ("[C]laims are read in light of the specification.") (citation omitted). And, as explained, the specification here specifically refers to ceasing processing *using the first rule set*

(*i.e.*, policy 130's rule set). Mot. at 19 (citing '806 Patent at 6:12-15, 7:25-32, 7:57-59, 8:4-23). Cisco has no answer for this. It asserts that Centripetal's reading "would produce absurd results," namely a scenario in which packets "pass through the system unexamined," Opp. at 17, but the asserted claims foreclose that result because they unequivocally require the application of at least one rule set. *See* '806 Patent at Claims 9 and 17 ("process, in accordance with the first rule set, a portion of the plurality of packets"). Cisco's arguments fail to defeat Centripetal's request to reopen proceedings to allow Centripetal to address the new construction—adopted by the Court for the first time in its Opinion—that "cease processing of one or more packets" does not mean stop processing packets with the old rule set.[9]

C. The Court Further Erred by Effectively Importing a Limitation From the Specification Into the Claims

Cisco does not dispute that a court may not import a limitation from the specification into the claims. Opp. at 19-20. Instead, Cisco tries to minimize the Court's improper comparison of the products to the specification as merely "support[ing]" the Court's conclusion. No matter how Cisco tries to spin it, the Court violated black-letter law by comparing Cisco's accused products to the '806 Patent's specification rather than to the asserted claims themselves. *See SRI Int'l v. Matsushita Elec. Corp. of Am.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985). Nor was this error "harmless." Opp. at 20. The Court's non-infringement finding was tainted by, and cannot be separated from, the Court's improper importation of additional limitations.

Cisco's attempt to revive Mr. Shankar's irrelevant testimony is unavailing. Contrary to Cisco's assertion, Mr. Shankar did not address the infringement scenario because he does not

[9] Cisco cites an unpublished opinion in *Intellectual Ventures II LLC v. Ericsson Inc.*, 686 F. App'x 900 (Fed. Cir. 2017) (*see* Opp. at 19), but it is inapposite. In that case, there was a "vigorous dispute" over the construction of the relevant term, 686 F. App'x at 904; here, by contrast, Cisco's own experts construed the relevant term in accordance with its plain meaning.

address Threat Intelligence Director providing rules to the firewalls or the fact the rules are preprocessed. Tr. 2518:22-2519:7 (addressing rule set programmed by a system administrator, not by a Firewall Management Center with Threat Intelligence Director that preprocesses and automatically distributes rules).

In sum, Cisco's opposition—which ignores Centripetal's arguments and its own source code, and misstates the evidence—does nothing to refute Centripetal's showing that an amended judgment of infringement (or an order reopening the judgment) is warranted to correct the Court's errors with respect to the '806 Patent.

III. THE '176 PATENT

A. There Is No Serious Dispute That Cisco's Evidence—Upon Which the Court Relied—Fails to Show Non-Infringement

Cisco's opposition fails to grapple with Centripetal's evidence—in the form of Cisco's own documents—showing that Cisco's Switches and Routers are able to generate and process ingress and egress NetFlow records and send them to Stealthwatch for correlation. Mot. at 23 (citing, e.g., PTX-591 at 522 (Cisco document stating that Stealthwatch collects NetFlow and WebFlow telemetry and correlates "both telemetry types")). Instead, Cisco merely points to the Court's order rejecting Centripetal's evidence, but does not dispute that both ingress and egress are collected, just that the ingress and egress are not necessarily compared because the egress may be ignored as an "error condition." [redacted]

Tellingly, Cisco acknowledges that its evidence—upon which the Court relied—"do[es] not foreclose the accused products" from infringing the '176 Patent in the manner alleged. Opp.

at 22. Accordingly, there can be no credible dispute that Cisco's evidence does not support the Court's non-infringement finding. And Cisco's assertion that Centripetal "does not refute" the Court's ruling that Centripetal failed to prove infringement is simply wrong. *See* Mot. at 23-25.

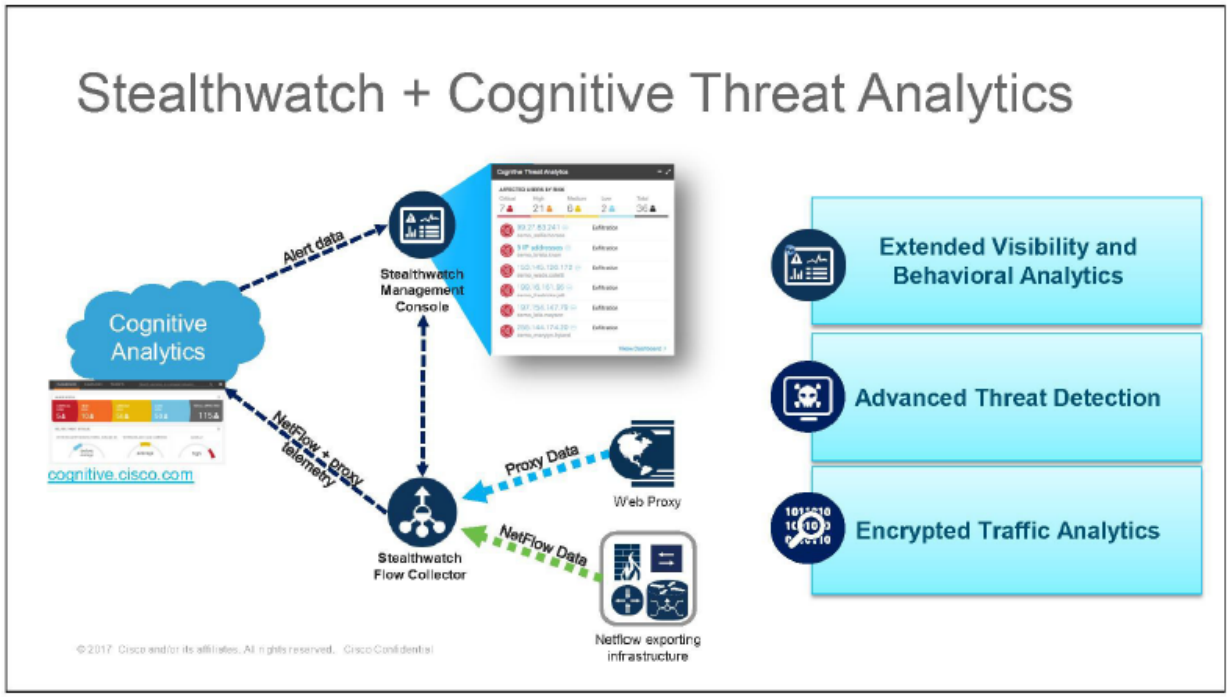
B. The Court Erred by Not Considering Deduplication and Proxy Technologies that Correlate

Centripetal showed that Cisco's deduplication technology infringes the '176 Patent, because all traffic within a network is sent to Stealthwatch and correlated in order to generate a Stealthwatch flow. PTX-569 at 3; *see also* R.63 Tr. 174:22-175:10; Dkt. No. 725 (Centripetal's FoF) at ¶¶ 351-352, 371. This flow is sent to CTA which allows the system to generate rules to prevent threats in the network. *See, e.g.*, PTX-1065 at 5; PTX-591 at 4; PTX-1009 at 9; PTX-989 at 33. Thus, contrary to Cisco's assertion that deduplication is irrelevant, *see* Opp. at 23-25, the correlation of traffic into and out of network devices to understand the network flow is essential to understand how to protect a network from malicious actors. *See, e.g.*, R.63 Tr. 177:14-178:1 (Dr. Almeroth confirming that during deduplication, ingress and egress flows are compared and deduplicated).

Cisco curiously argues that this is a new theory. Opp. at 23. But Centripetal's infringement position has always been that Stealthwatch performs correlation. *See, e.g.*, Tr. 994:22-995:8. Cisco's attempted rebuttal is built on a simple misunderstanding of Centripetal's infringement case, where Centripetal properly alleged deduplication meets this element. Dkt. No. 725 (Centripetal's FoF) at ¶¶ 350-352, 371; PTX-1060 at 23 (showing the comparison of egress and ingress logs for deduplication); *see also* Tr. 983:14-987:2. In light of that misunderstanding—and because the evidence demonstrates that deduplication further shows that Stealthwatch correlates log entries—Cisco's opposition fails at its threshold.

Centripetal also showed that proxy data is correlated to generate a Stealthwatch flow. *See, e.g.*, Tr. 1115:2-1116:20, 985:1-8, 996:17-999:5 (Dr. Cole testifying that Stealthwatch correlates proxy data including WebFlow and Syslog); PTX-591 at 4. Cisco attempts to muddy the waters arguing that Syslog/WebFlow are not log entries, Opp. at 25, but it is well known that "syslog" stands for "system log" and is a log *by definition*, *e.g.*, Tr. 1115:2-21 (Dr. Cole describing the fields of the Syslog). Thus, because there is no credible dispute that a syslog contains log entries, Cisco's defense that the Syslog/Webflow do not meet the log entry element of the claims falls apart.

Cisco's opposition ignores Centripetal's showing that proxy data represents traffic that enters and leaves a switch or router. Tr. 1115:2-1116:20. As shown in the figure below, a proxy receives data that is transmitted from and received from a router:



This solution uses the Proxy ingestion feature to consume Syslog information sent from proxy sources, integrating it into Stealthwatch's flow visibility.
Supported integrated proxies
Cisco WSA
Bluecoat proxy
Squid
McAfee Web Gateway
will provide information about observed Web traffic reported, and send it through syslog to the Flow Collector.
This syslog information contains details similar to what a flow record contains: Source IP, destination IP, Source Port, Destination Port, URL, Username.

Stealthwatch will then correlate the received syslog and relates it to the flows collected from network devices before and after the proxy, providing deeper visibility into customers web traffic.

Customer may use either NetFlow or Proxy data, or both. The netflow data sent into the Cloud consists of perimeter traffic, telemetry corresponding to traffic occurring between inside and outside host groups.

PTX-1065 at 5 (excerpted).

This data is fed into Stealthwatch which correlates to the log entries in order generate a Stealthwatch flow. *See* Tr. 1115:2-1116:20, 985:1-8, 996:17-999:5. Accordingly, Cisco's own documents prove that proxy data is correlated and is another basis for infringement.

C. Cisco Does Not Dispute that Limitations May Not Be Imported to the Claims, or that Centripetal's Evidence Could Establish Obfuscation

The Court's understanding of "correlation" (and attendant finding of non-infringement) violated black letter law because it was informed by the limitation from the specification requiring that the accused products address the issue of "packet obfuscation" Op. at 53-59; *see SRI Int'l.*, 775 F.2d at 1121. Cisco tries to minimize this error by claiming that the Court's importation was immaterial to the Court's opinion. Opp. at 27. Cisco is wrong. As Centripetal explained in its Motion, Centripetal could have satisfied the Court's new packet obfuscation requirement (had it been afforded proper notice) with evidence of that the accused products can perform functionality like NAT. *See e.g.*, Mot. at 28. Cisco does not dispute that the accused products could perform NAT translations and that they would have satisfied the Court's "packet obfuscation" requirements. *See* Opp. at 27-28. Instead, Cisco makes the unremarkable observation that NAT is a new theory. Of course it is; Centripetal had no notice that it needed to advance a theory to

establish obfuscation under the Court's new construction.

Ultimately, Cisco does not dispute that a party must be afforded proper notice of a court's new claim construction. If the Court declines to amend its judgment to rule for Centripetal, then it should reopen it to permit Centripetal to establish infringement under the new construction.

D. The Court Erred in Concluding that the Accused Products Do Not Generate and Provision Rules in Response to Correlation

Centripetal presented evidence that Stealthwatch with CTA does "generate[], based on the correlating, one or more rules configured to identify packets received from the host located in the first network" or "provision[] a device" with those rules. In particular, Dr. Cole identified that at "Step 0" of PTX-1089 at .1238, that Stealthwatch generates and "send a policy, which can also be thought of as rules, to take some action, in this case to quarantine a specific IP address." Tr. 1002:4-1003:1.[10] Dr. Cole further explained that Cisco's Stealthwatch document further shows a policy (*i.e.*, rule) generated and provisioned to a device. Tr. 1004:20-1005:19 (citing PTX-595 at 25-26 (which shows an active policy with rules (the "ANC_Investigate" policy) for the host IP address (10.1.100.101)). Thus, Stealthwatch with CTA generates a policy update that is a rule because it includes a condition in the IP address of the host computer that will cause the function of quarantining a host computer. PTX-1089 at .1238 (showing "Quarantine" function is applied to packets with the condition of having IP Address 10.123.1.101, which is the output of Step 0). The rule can be sent automatically by Stealthwatch using pxGrid and ISE ANC. PTX-1089 at .1238 ("ANC can be invoked via pxGrid 1.0 or pxGrid 2.0 API"); PTX-1326 at 11 ("[Y]ou can manually or automatically change your users' access privileges when there's suspicious activity,

[10] Cisco also confusingly argues "CTA alerts" are not addressed in Centripetal's Motion. Opp. at 28. CTA alerts are part of the process of generating rules as it identifies the malicious IP address for Stealthwatch to generate a rule to send to ISE. PTX-584 at 062403 (showing CTA alerts and noting that "malicious encrypted flow can be blocked or quarantine by Stealthwatch").

a threat, or vulnerabilities discovered. . . . Upon detecting a flagrant threat on an endpoint, a pxGrid eco-system partner can instruct ISE to contain the infected endpoint either manually or automatically.").

Cisco fails to rebut the evidence cited by Dr. Cole that the functionality and the device that generates and provisions the quarantine rule is Stealthwatch, which is shown in "Step 0" of PTX-1089 at .1238-39 (showing Stealthwatch identifying the suspicious host, generating a policy rule of "quarantine" by default, and "send[s] . . . assignment request to ISE"). Cisco confuses the infringement scenario by pointing to "Step 1", which is "Apply ANC Policy 'Quarantine,'" and argues that it requires user intervention to "notice the alert." Opp. at 28-29. However, the user intervention is irrelevant to the issue of whether the system or the computer readable medium has the capability to generate and provision the rule because it is Stealthwatch's functionality that generate and provision rules in the infringement scenario. If an administrator wanted to write rules for the accused products, it could do so with directly connecting to accused Switch or Router and using its user interface. Cisco failed to show a user interface in Stealthwatch that is specifically used for generating rules. Indeed, Cisco conclusorily states that PTX-595 at 25-26 shows that the human generates the rule, but that exhibit states no such thing. Opp. at 29. Rather, it shows a default rule in place ("ANC_Investigate") that can be changed by the administrator with the "Edit" button. [redacted]. Tr. 1000:18-1001:7 ([redacted] citing PTX-1849 at 7 (line 13)). He also pointed to an internal Cisco document that shows the output of Step 0 is a rule (policy) to quarantine the host. PTX-1089 at .1238. While the administrator can select other options for the rule using the "Edit"

functionality, it does not change the fact that Stealthwatch has the capability of generating the rule in the first place and provisioning the rule to a device. Furthermore, pxGrid can also be used to provision the rules to devices automatically. PTX-1089 at .1238; PTX-1326 at 11; *see also* PTX-989 at 33. Cisco is unable to dispute the fact that Stealthwatch's functionality is what generates a rule and provisions a device, not the administrator.

Cisco's arguments in the last two paragraphs of its brief are irrelevant to Centripetal's arguments. Centripetal's argument is that a "rule" is created by the Stealthwatch software and not that a "rule" is embedded software in Stealthwatch. Opp. at 29-30. This is consistent with the claim's requirement of "memory storing instructions that when executed . . ." will "generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network." '176 Patent at Claim 11. Cisco's argument that the ANC policy updates do not "identify packets" is similarly misplaced because, as Centripetal described in its Motion at 28, the IP addresses in these updates identify those packets through the IP address of the sending host, making Cisco's argument irrelevant. Opp. at 30. Centripetal specifically called out this IP address shown in PTX-1089 at .1238 as identifying the host that sent the traffic. Mot. at 28-29.

Accordingly, the Court erred in finding non-infringement because Cisco's products correlate as set forth in the claims because they compare ingress, egress, and proxy data, as well as perform deduplication. Additionally, Cisco's products provision rules in response to this correlation using ANC policy updates to quarantine infected host computers inside the customer's network.

CONCLUSION

For any and all of the foregoing reasons and those set forth in Centripetal's Motion, Centripetal's Motion should be granted.

Respectfully submitted,

Dated: March 28, 2024

By: */s/ Stephen E. Noona*

Stephen Edward Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 W. Main St., Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Paul J. Andre (*pro hac vice*)
Lisa Kobialka (*pro hac vice*)
James Hannah (*pro hac vice*)
Hannah Lee (*pro hac vice*)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
hlee@kramerlevin.com

ATTORNEYS FOR PLAINTIFF CENTRIPETAL NETWORKS, LLC

CERTIFICATE OF SERVICE

I hereby certify that on March 28, 2024, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will automatically send notification of electronic filing to counsel of record.

/s/ Stephen E. Noona
Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com